

100

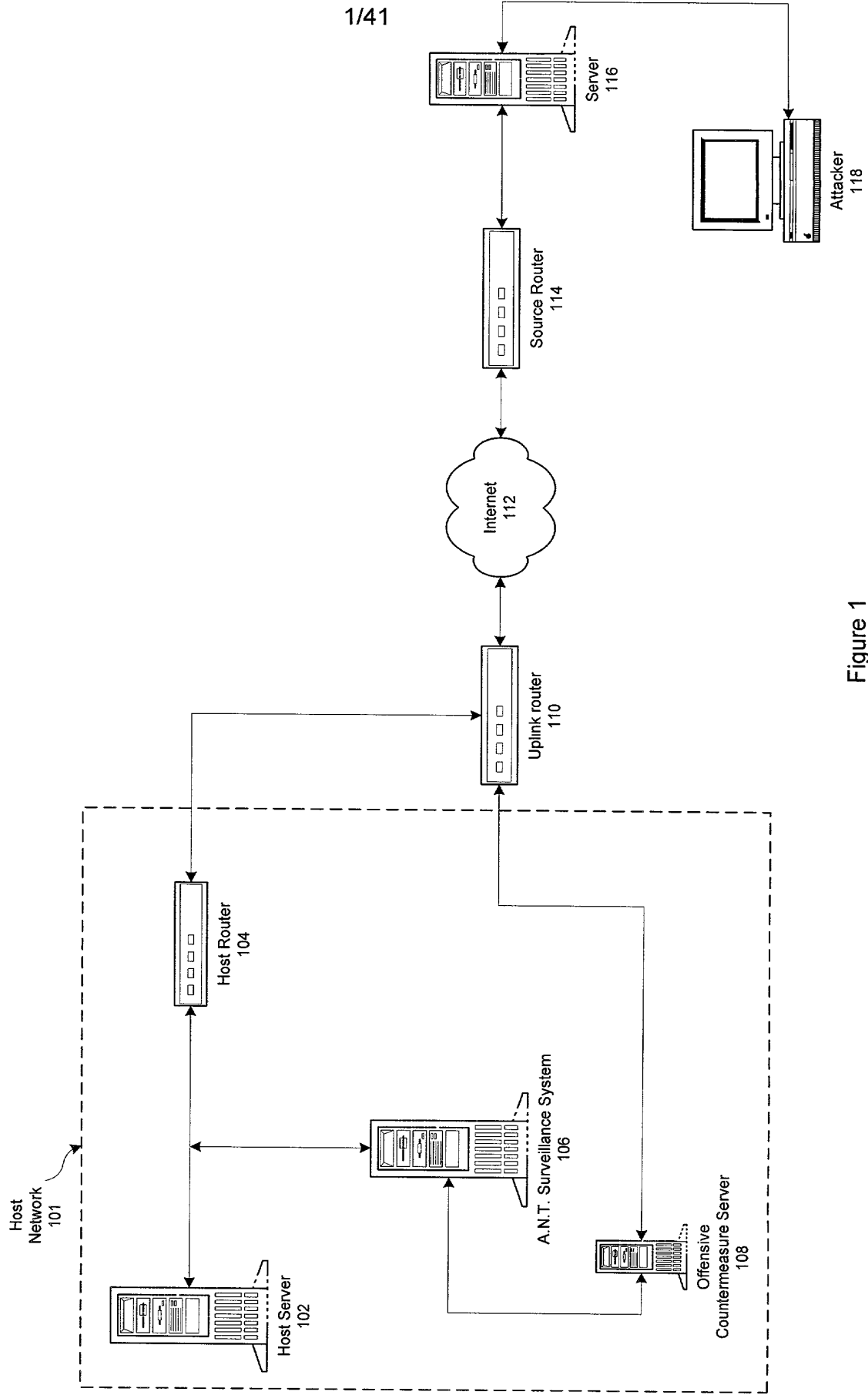


Figure 1

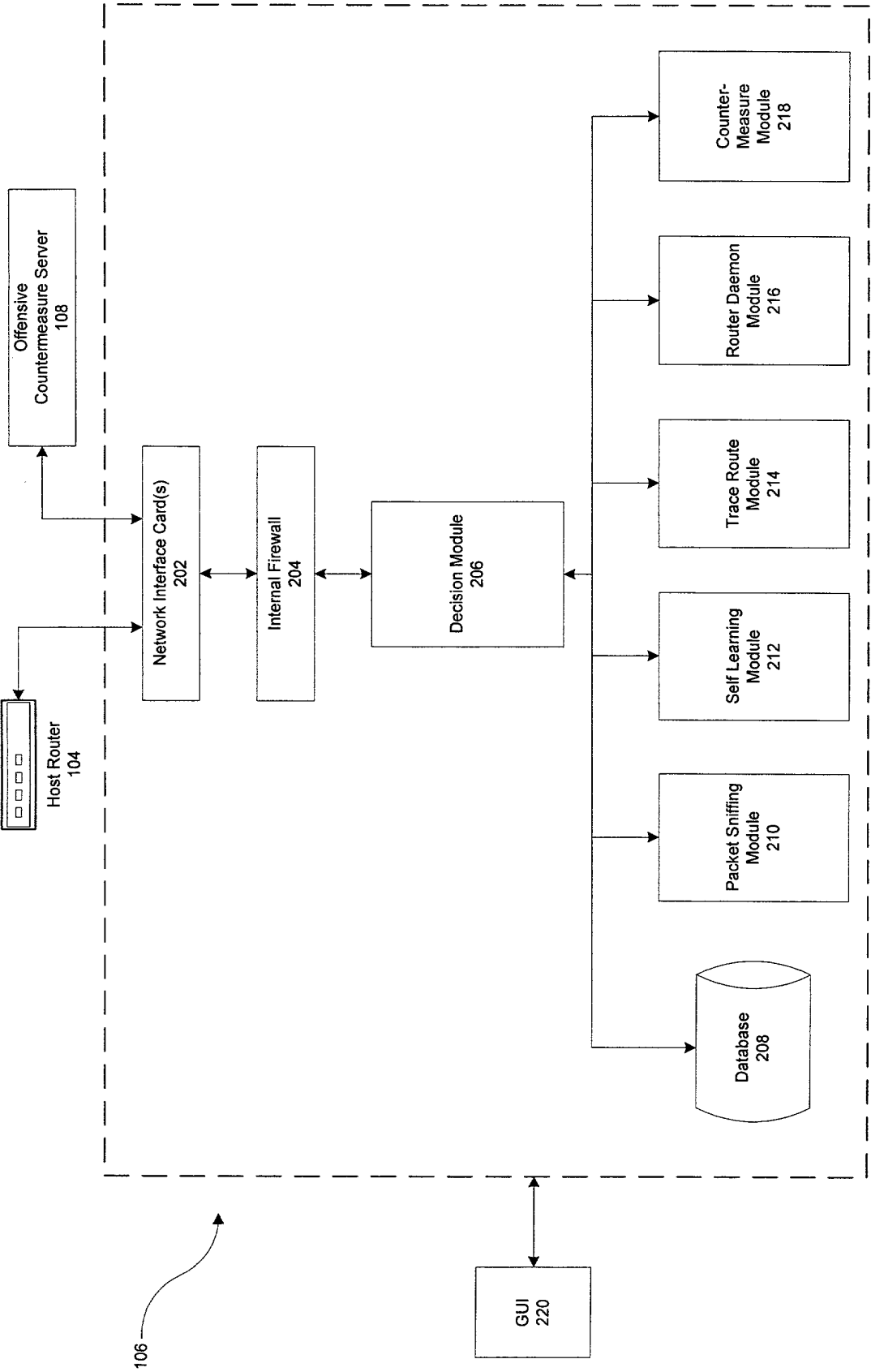


Figure 2

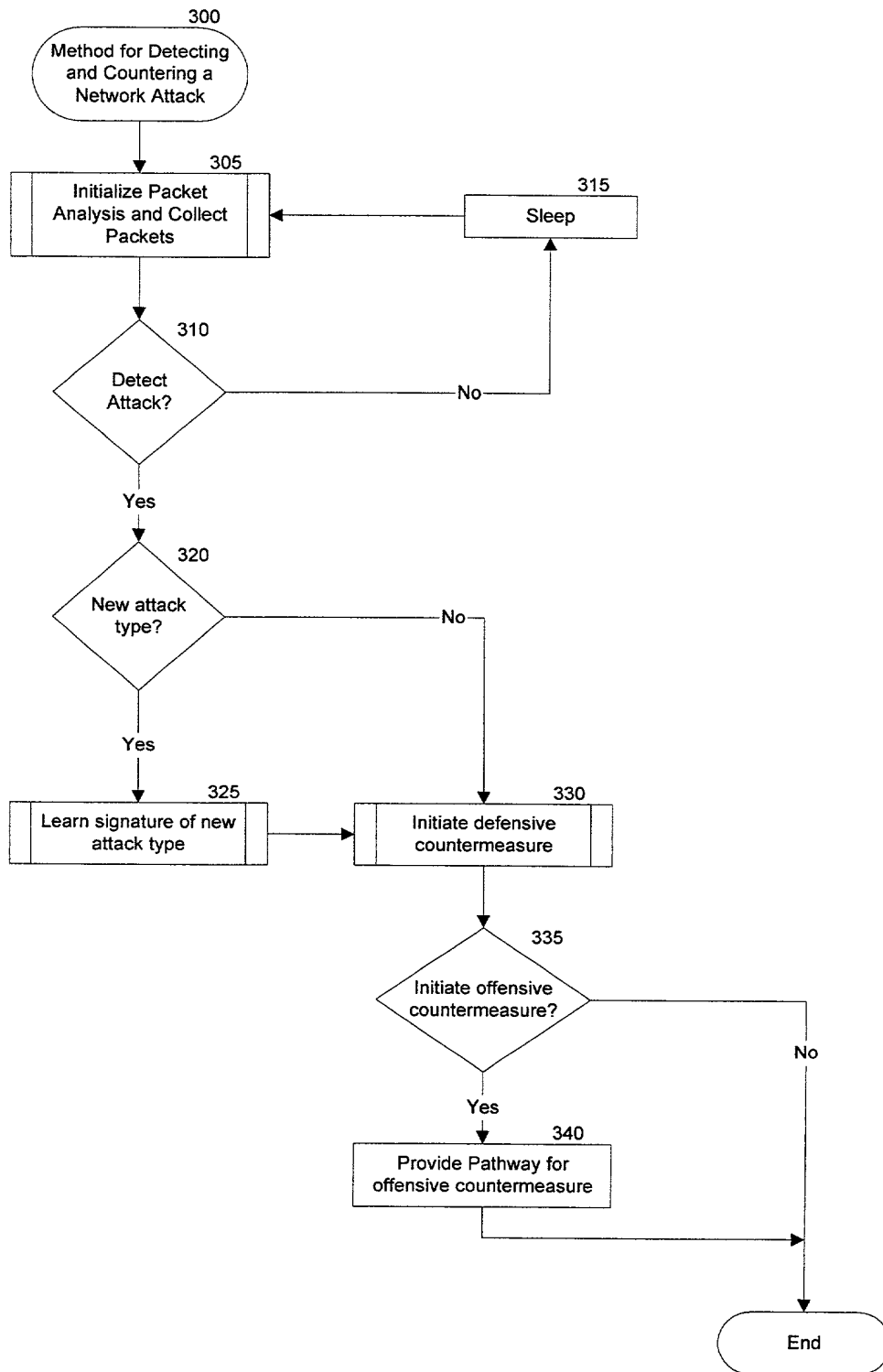


Figure 3

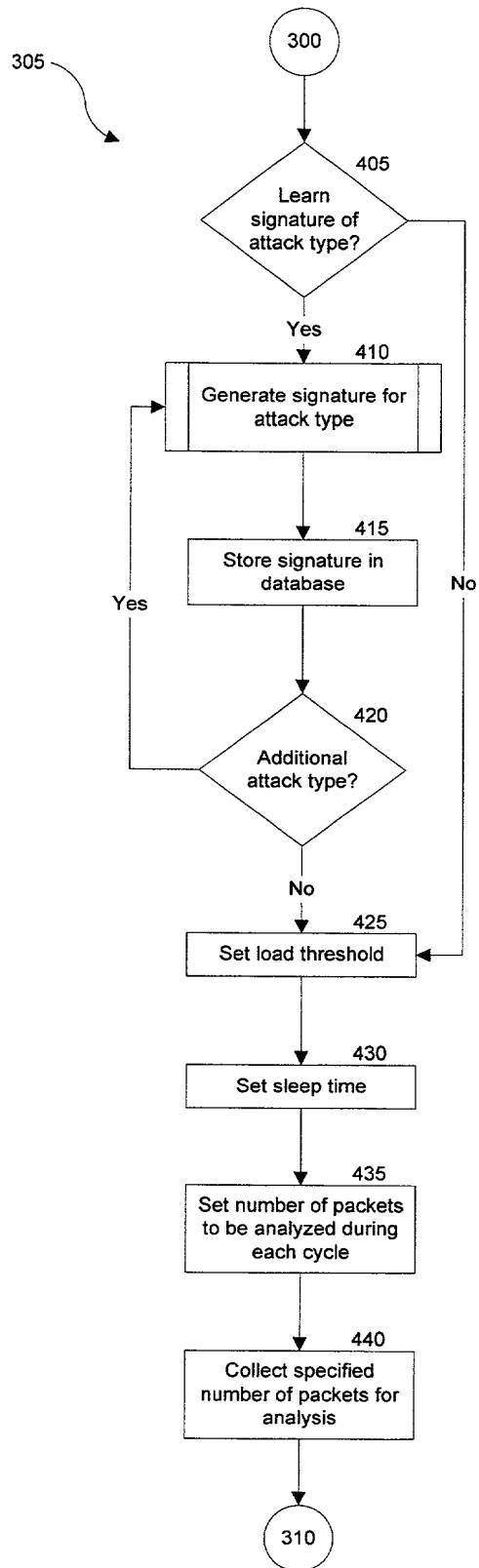


Figure 4

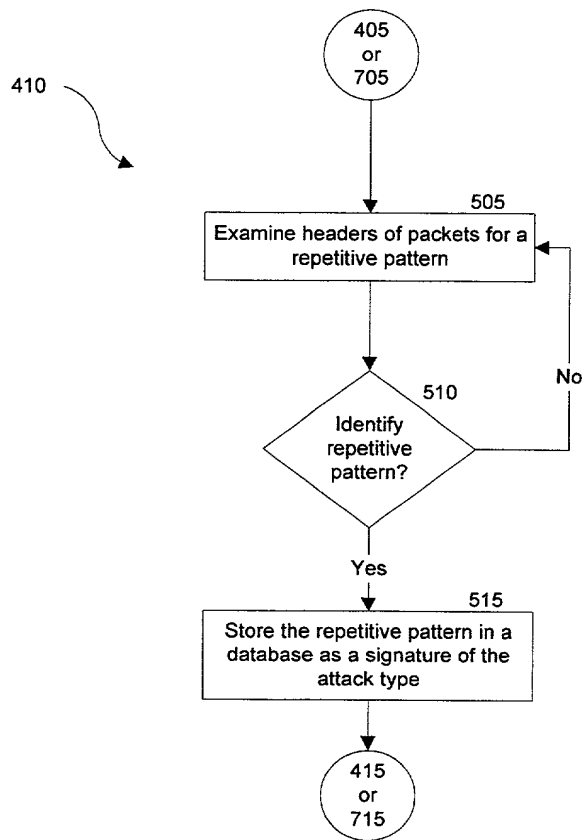


Figure 5

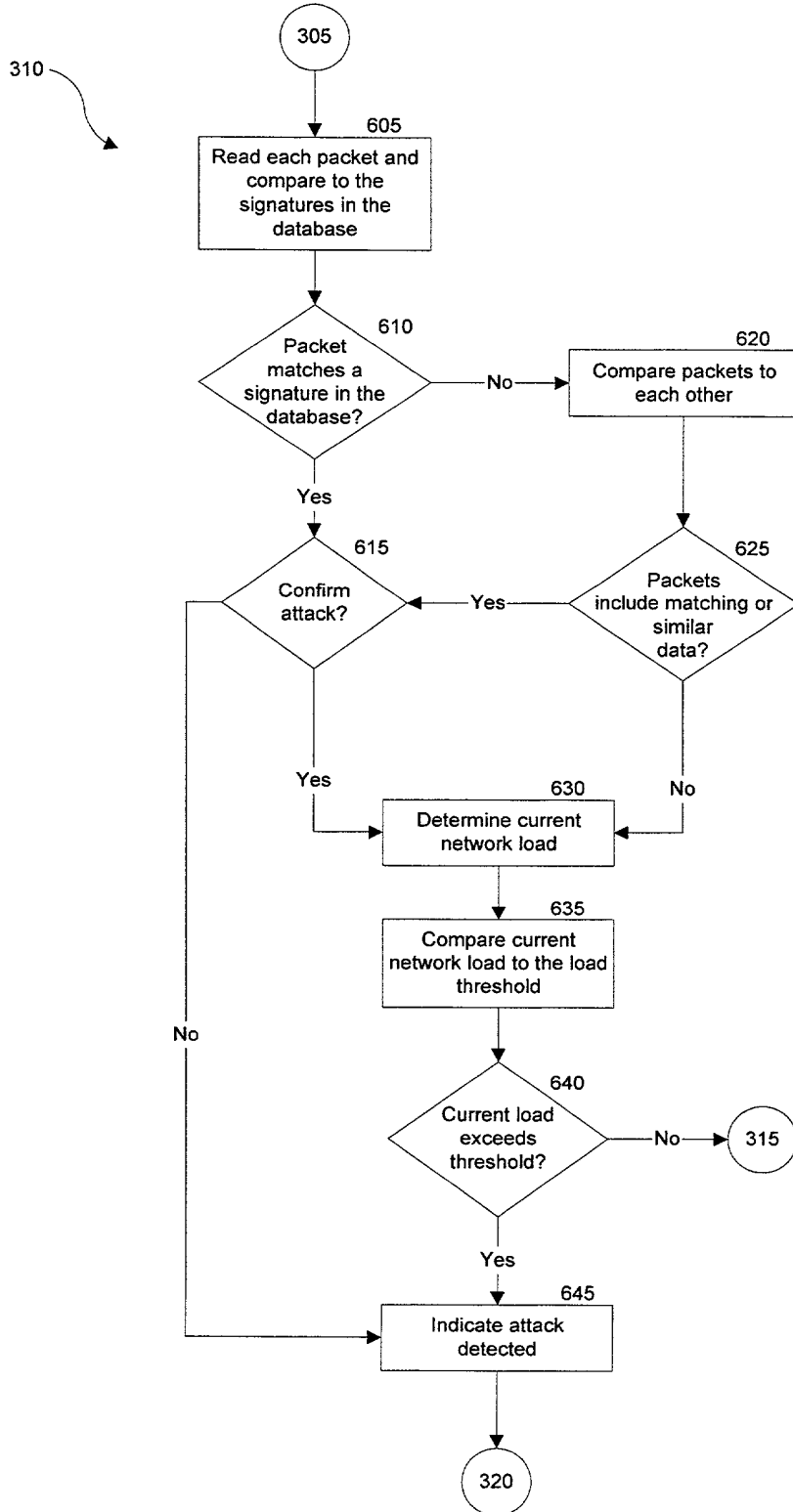


Figure 6

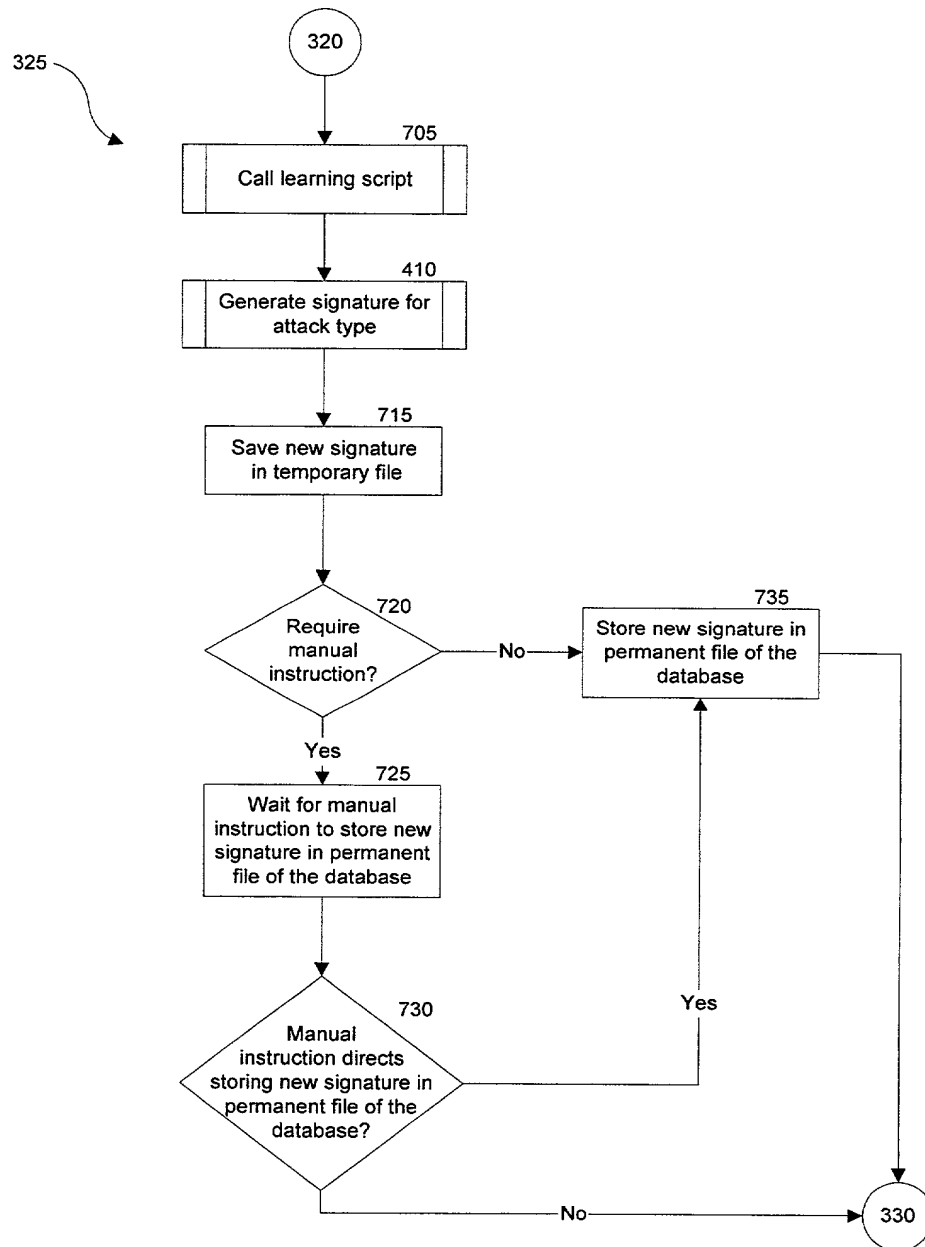


Figure 7

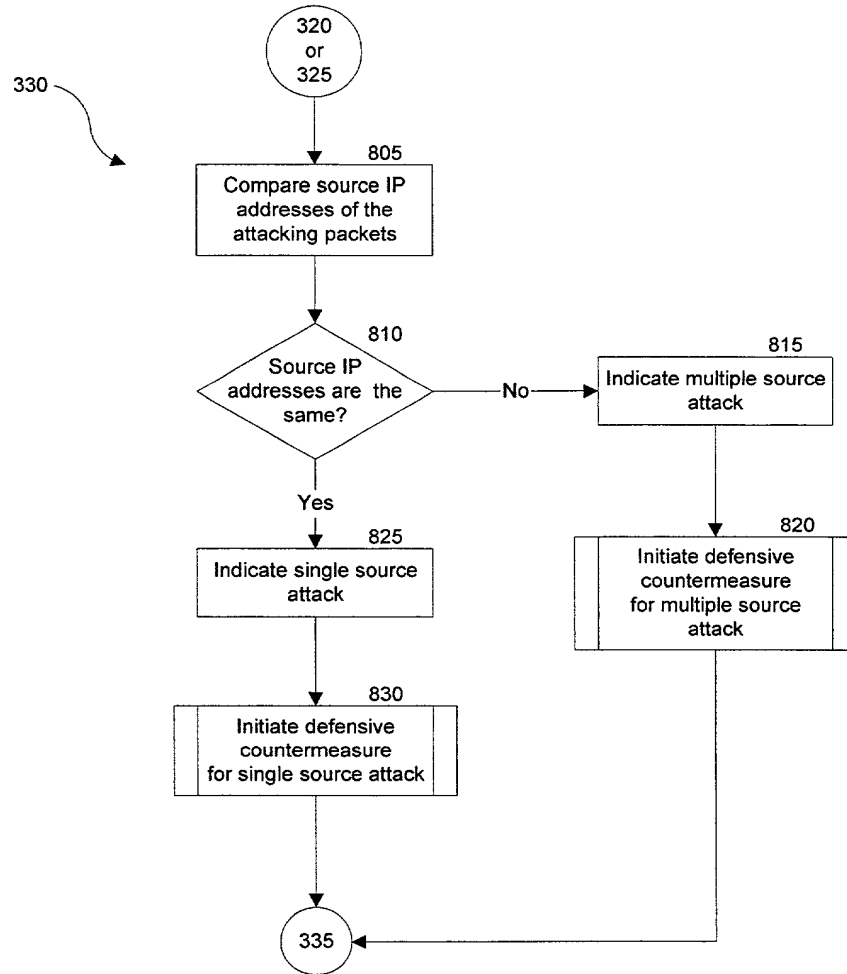


Figure 8

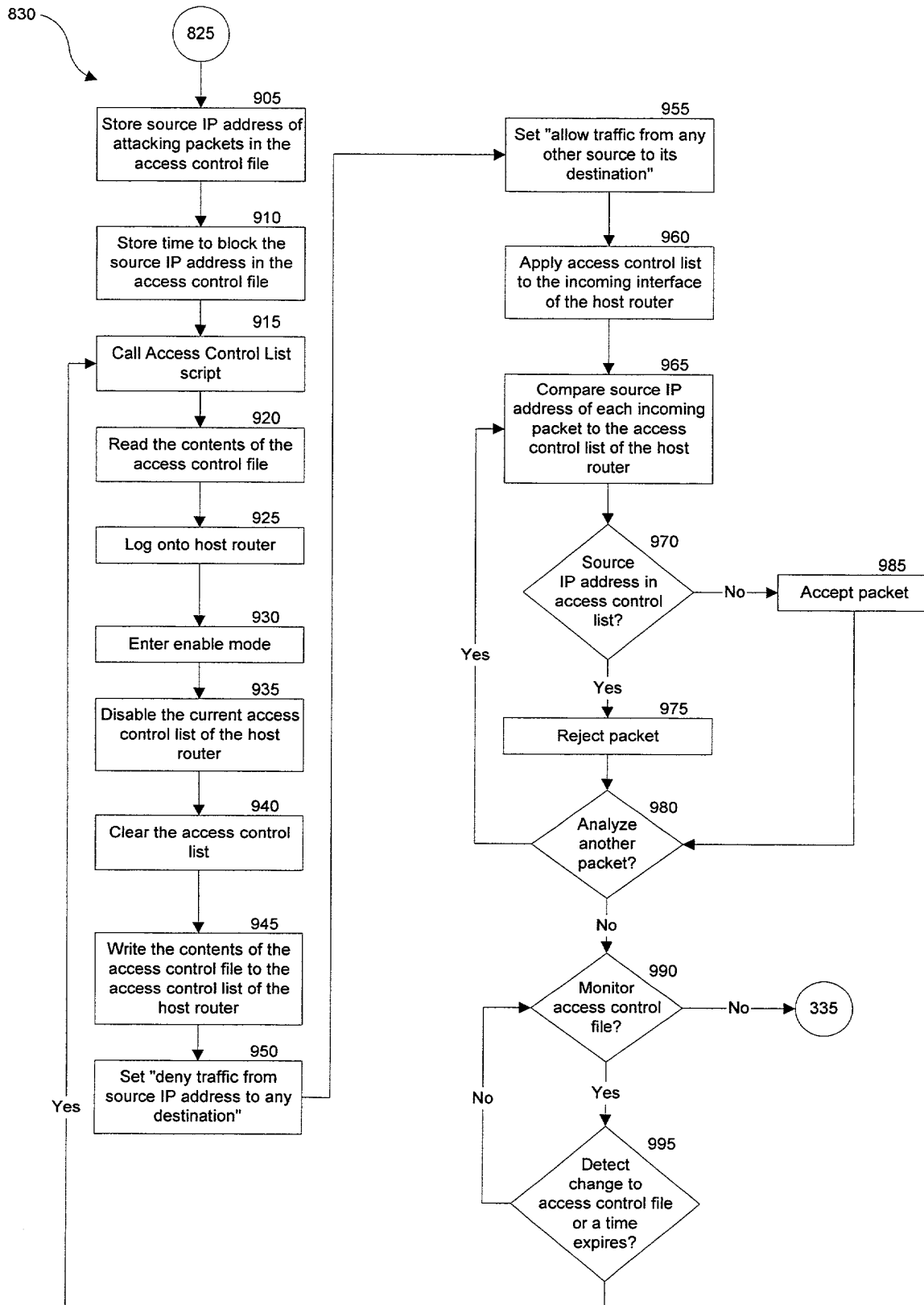


Figure 9

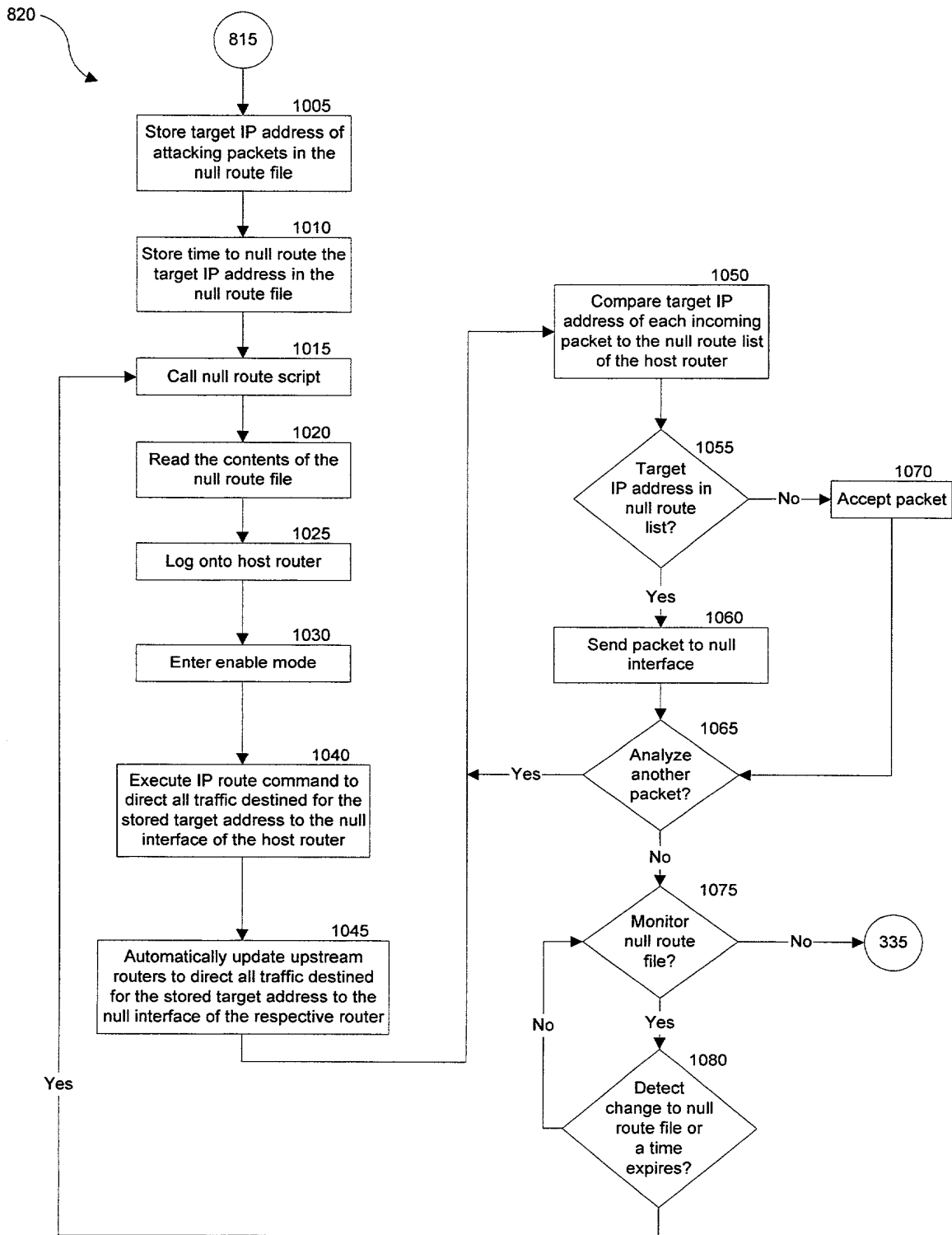


Figure 10

1100

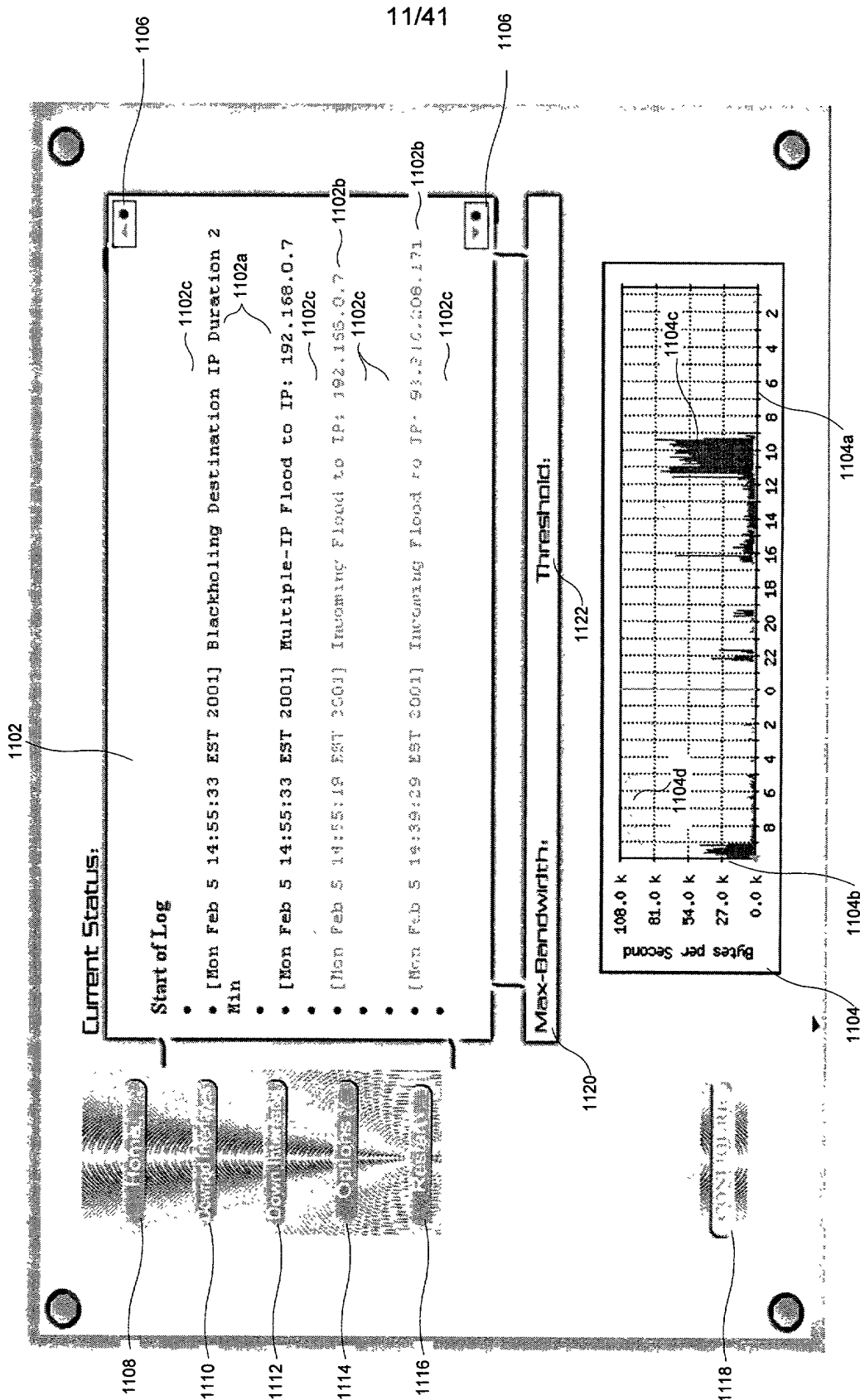


Figure 11

1200

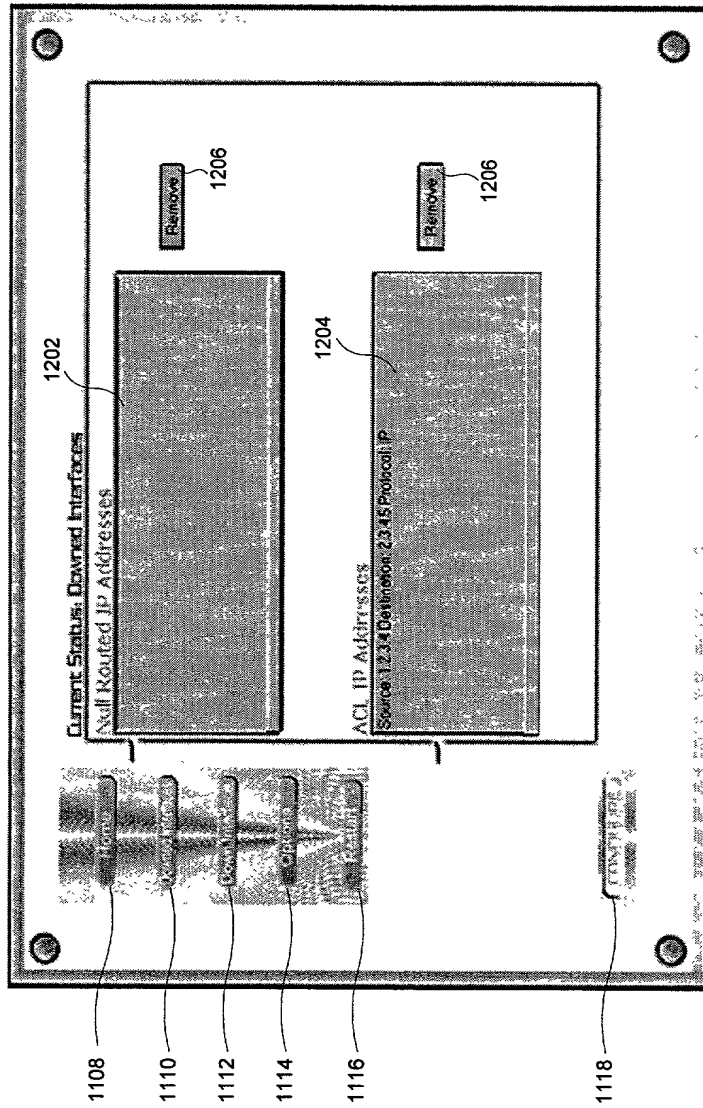


Figure 12

1300

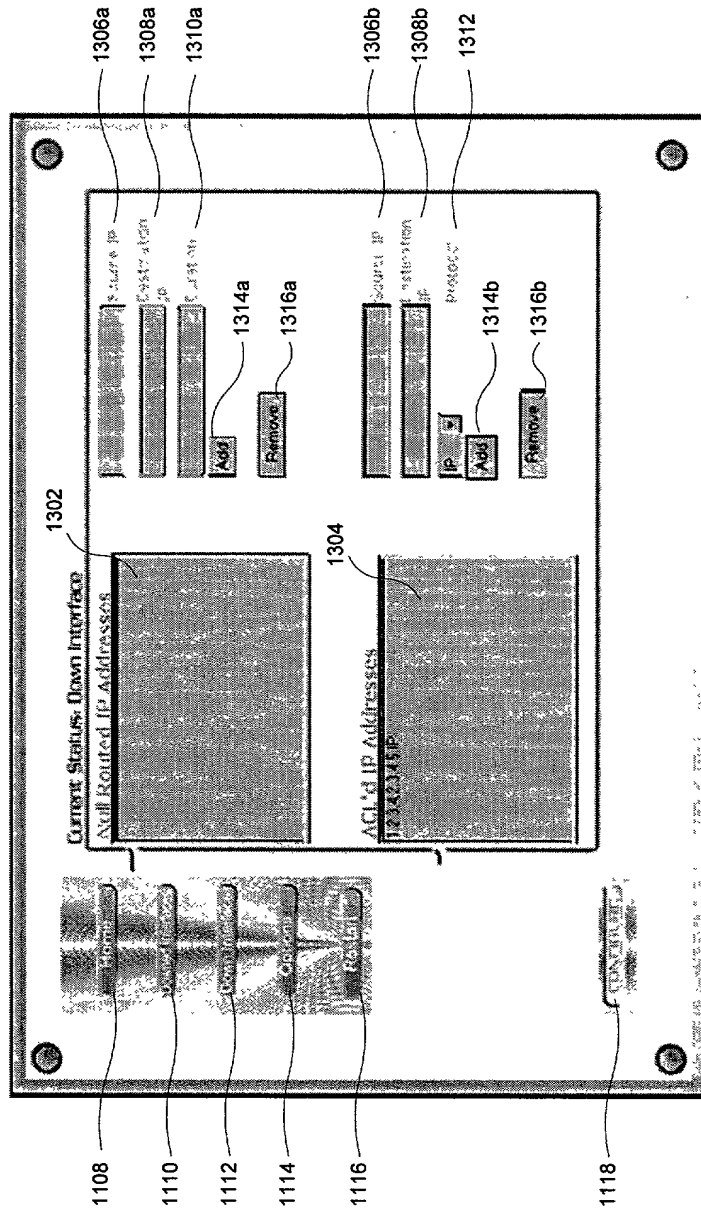


Figure 13

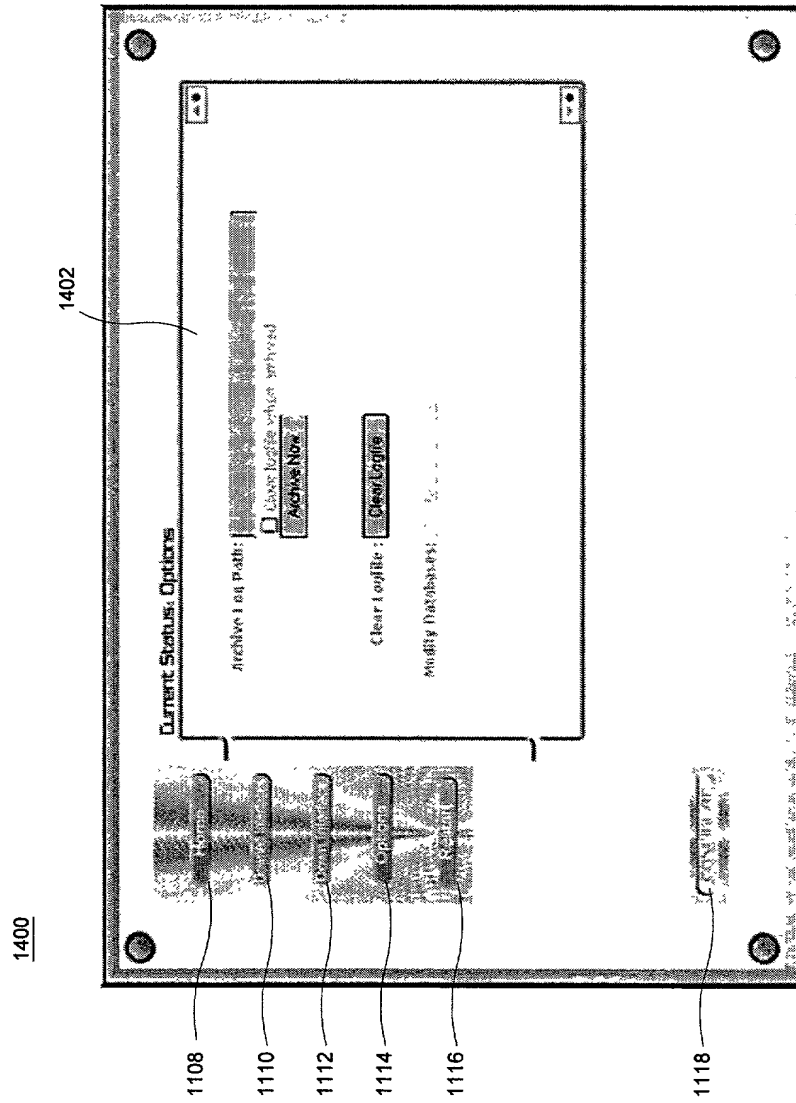


Figure 14

1500

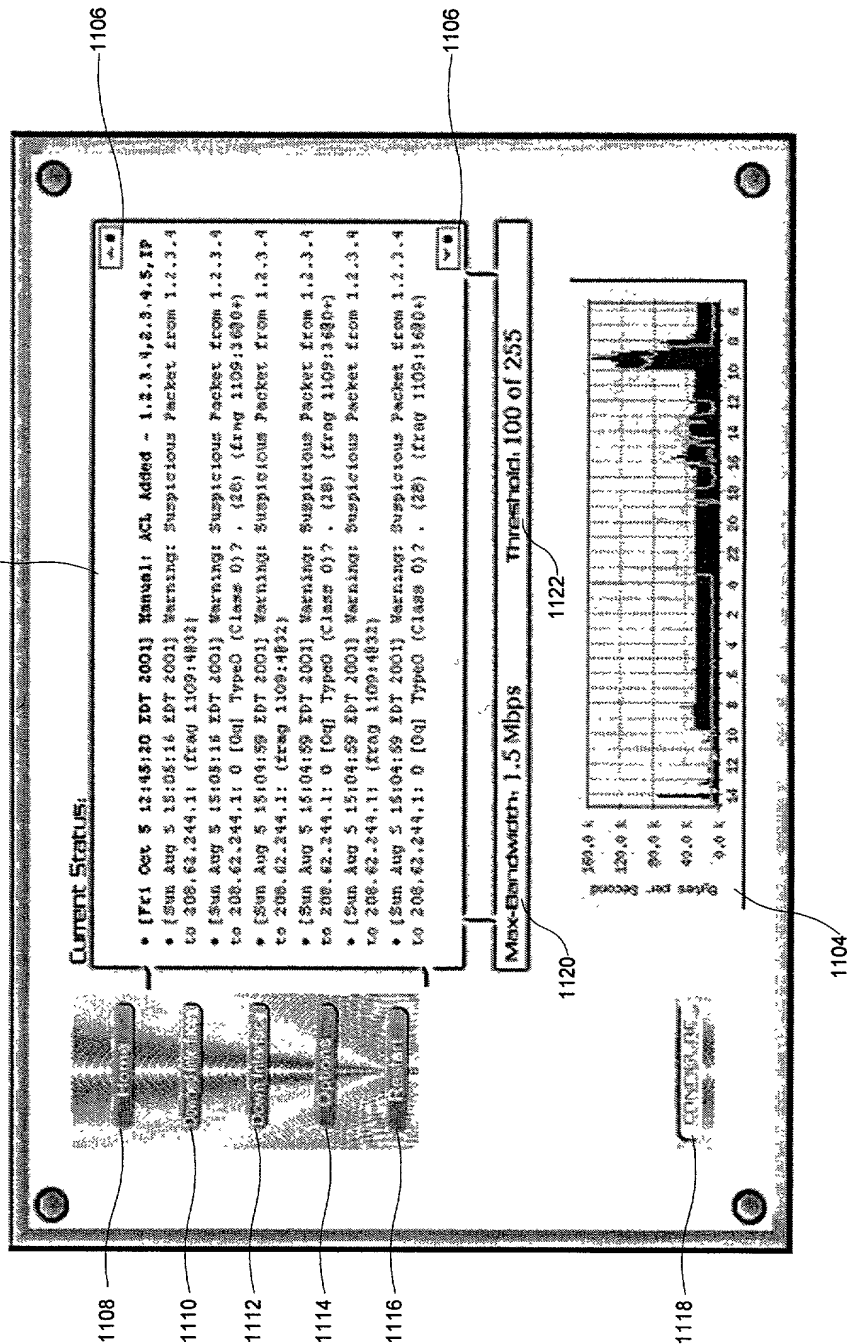


Figure 15

1600

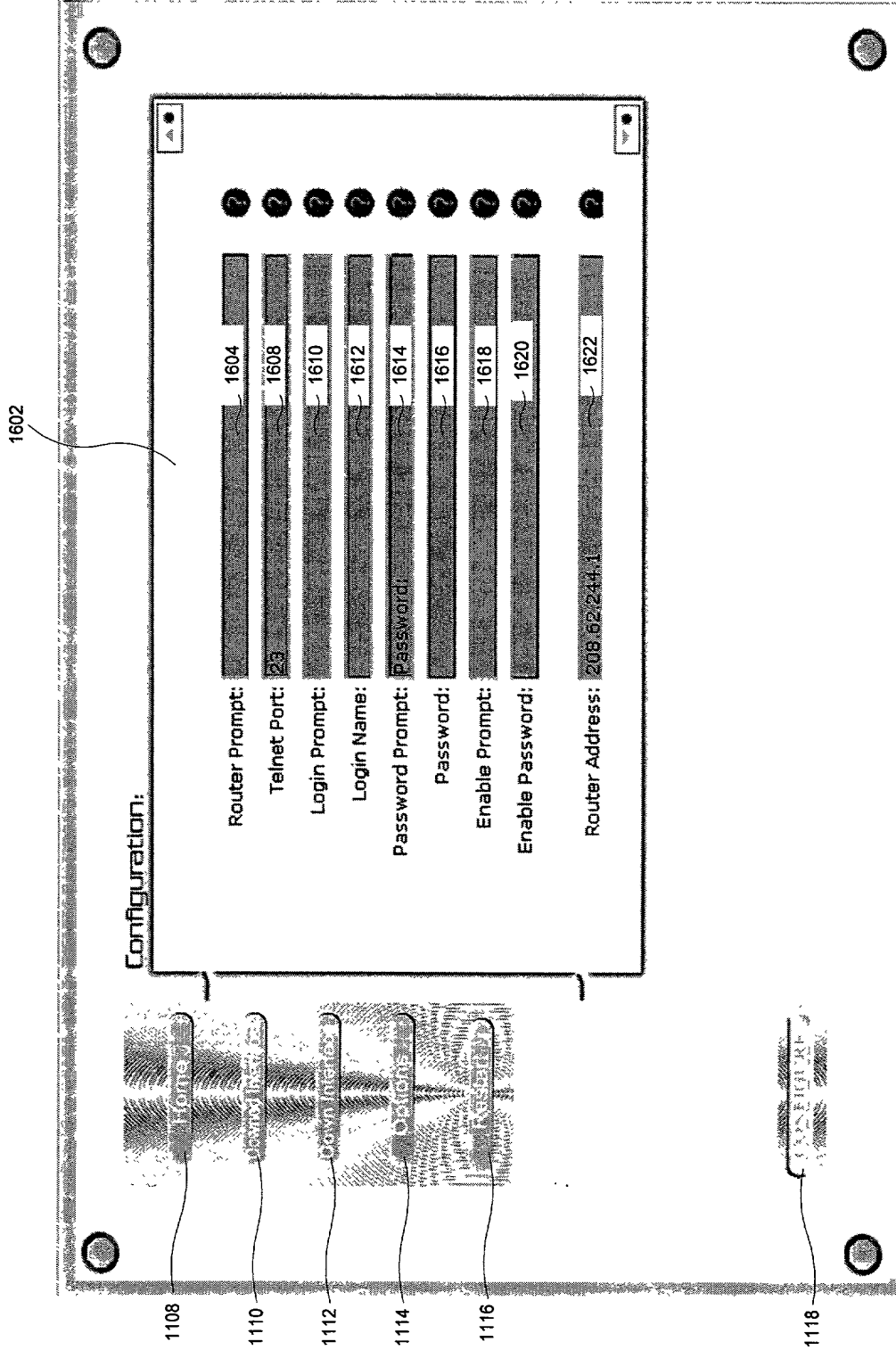


Figure 16A

1600

1602

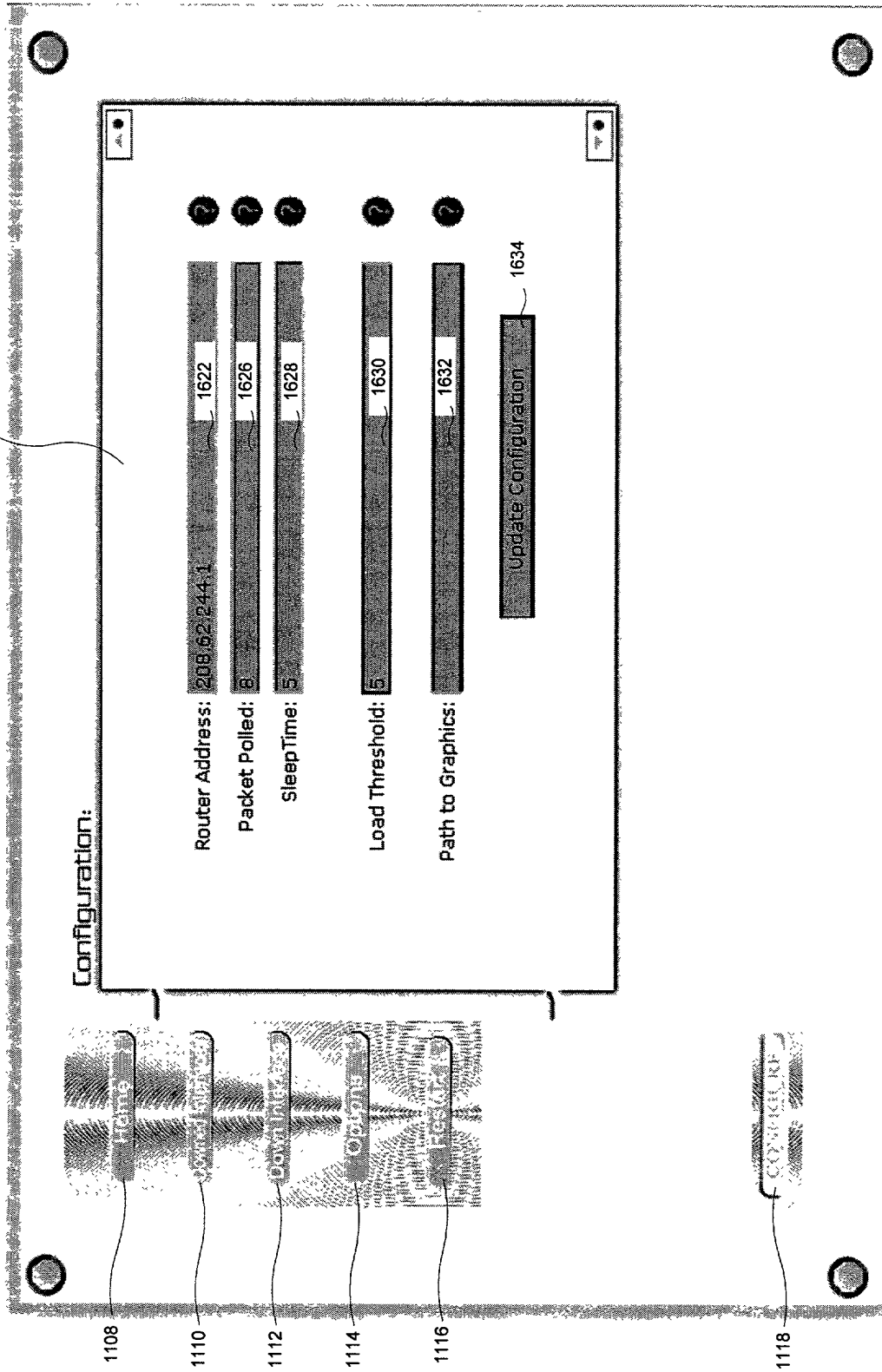


Figure 16B

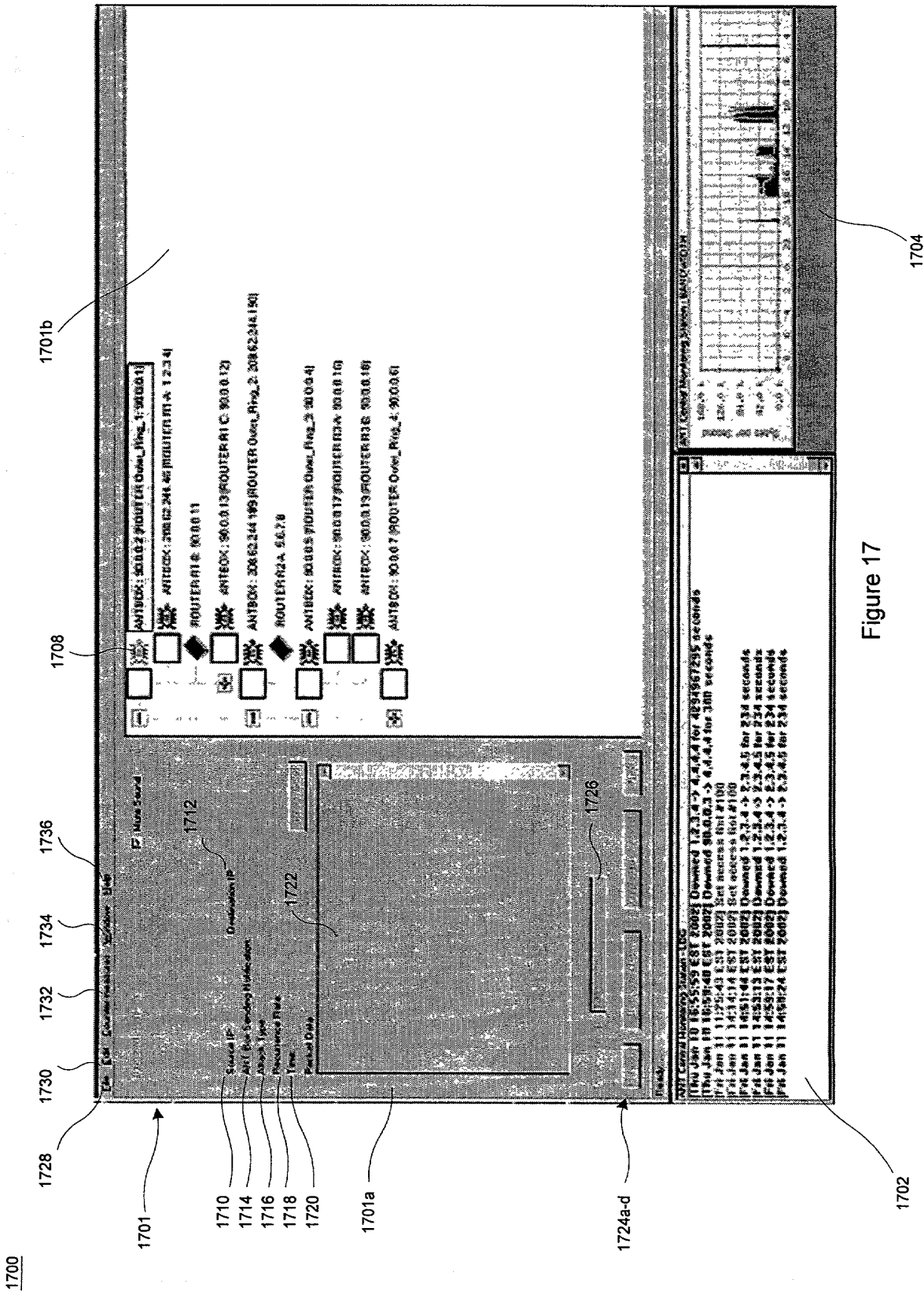


Figure 17



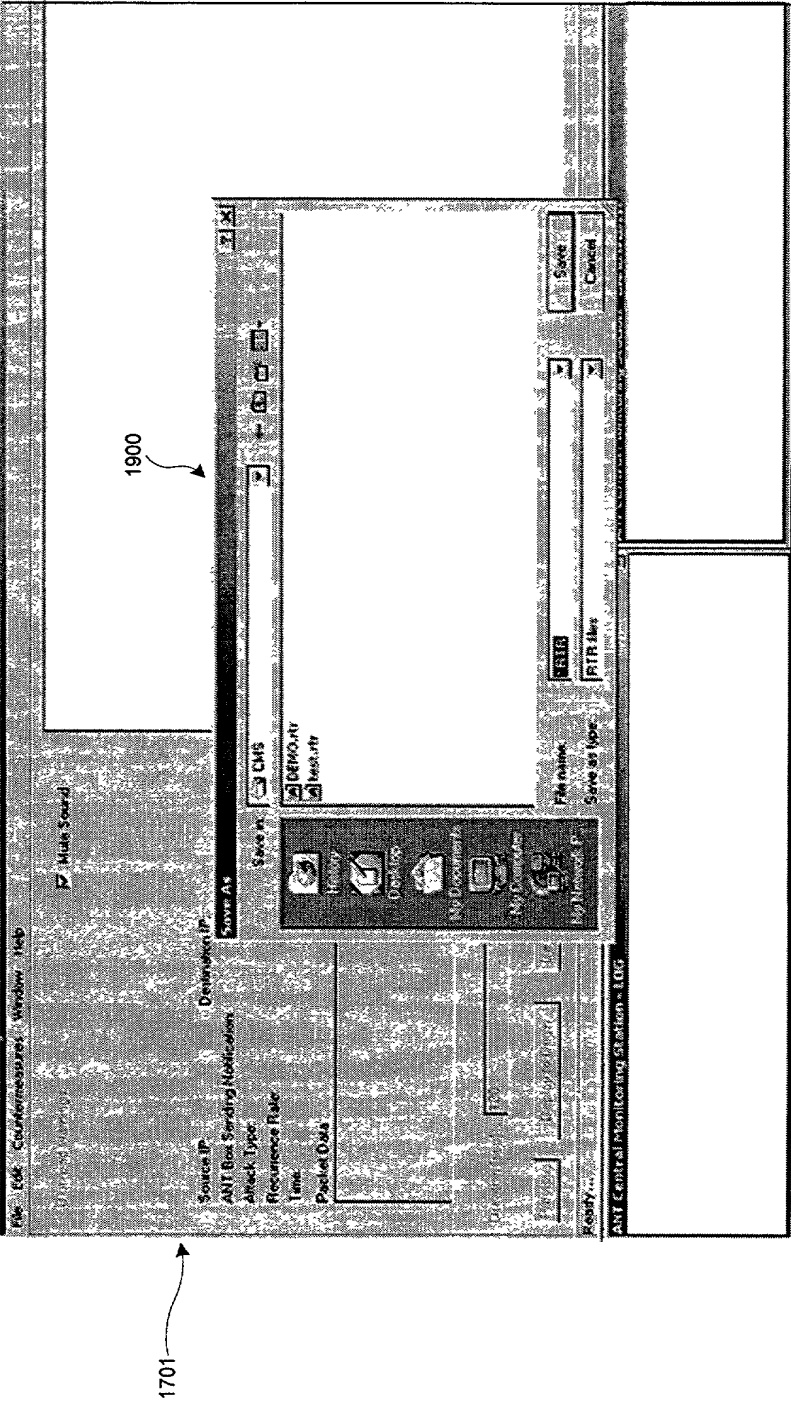


Figure 19

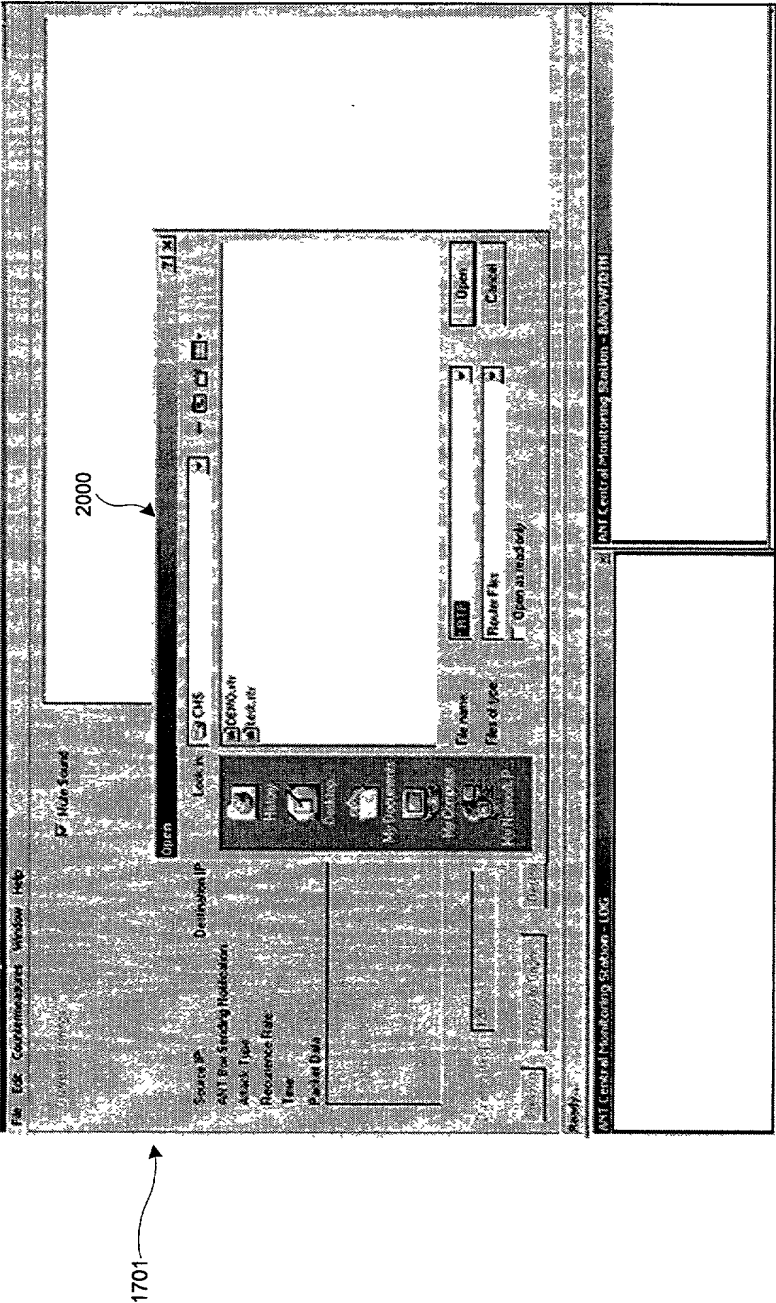


Figure 20

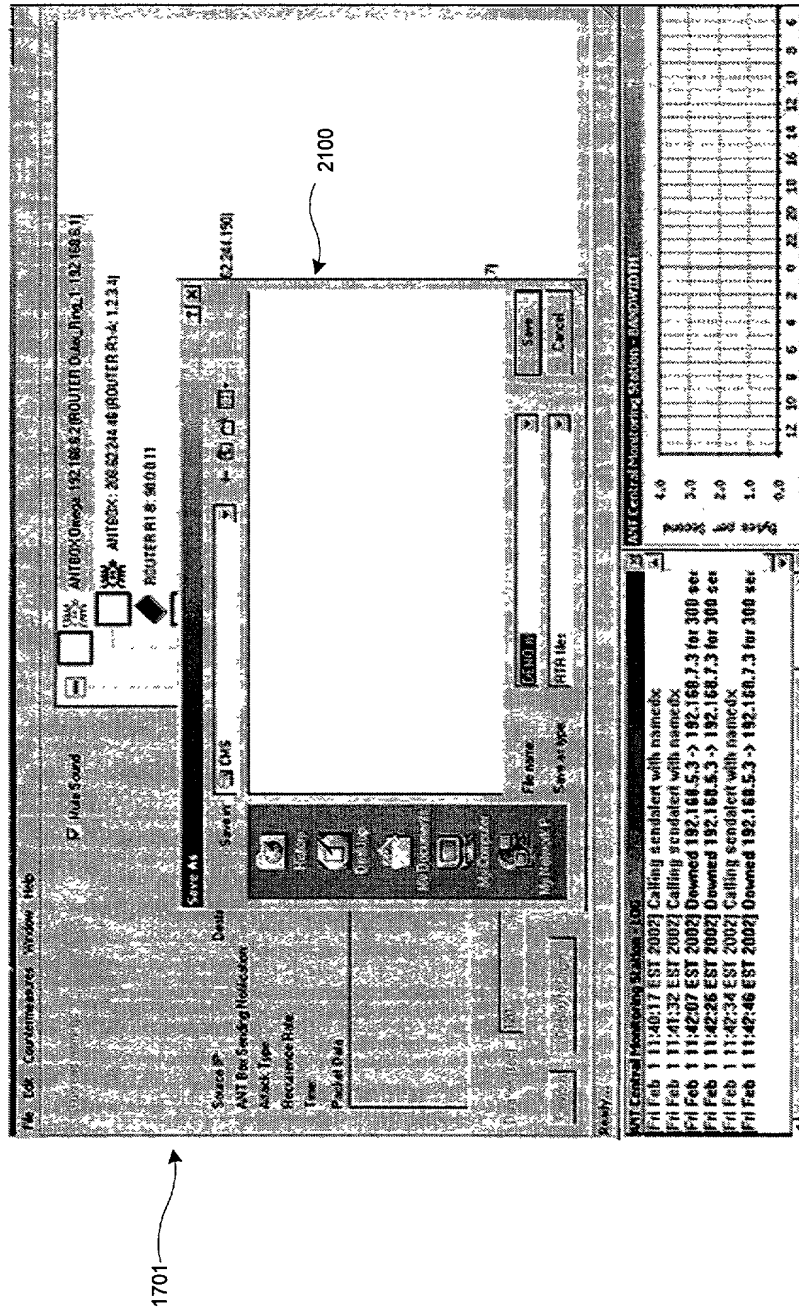


Figure 21

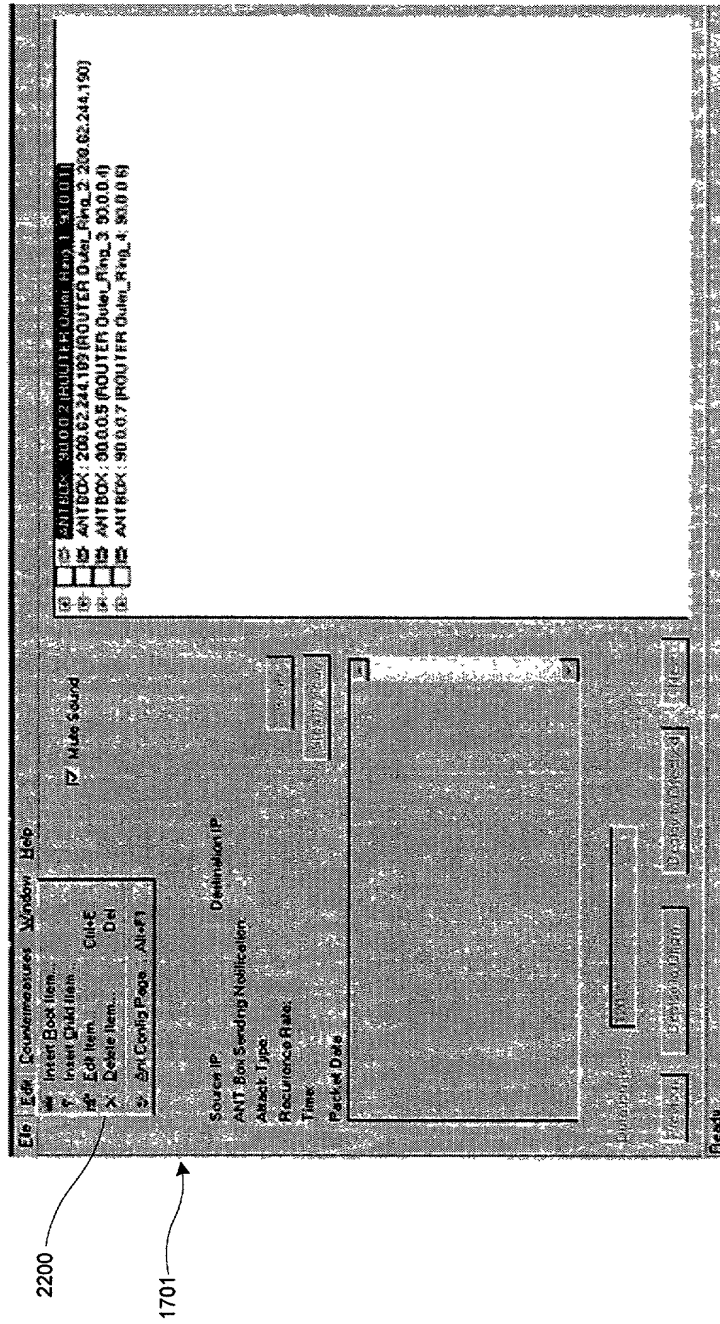
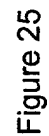


Figure 22







2600

Mode:

Threshold (0 to 255):

Packets/sec Threshold:

Sleep Cycle (s):

Router Login:

Password:

Enable Password:

Black hole duration (min):  
Uz:   
Them:

Recurrence Rate:  Packets Per Cycle:

Other items:  
wav=No  
wav\_path=wav/alert.wav  
noscriptpath=cisco.nonull  
routermanpath=/home/tanlon/an/cms/routeman.pl  
adscriptpath=cisco.ad  
scriptpath=cisco.null  
iswitch=isp0  
itacet=0  
cndpath=/usr/home/sysadmin/web/test.cmd  
aclint=serial0/0.1  
noroute\_path=/usr/home/sysadmin/web/noroute  
mainrefresh=30  
threshold\_interface=serial0/0  
AniHost=208.62.244.46  
RouterAddress=208.62.244.1  
TelnetPort=23

OK

Cancel

Figure 26

2700

1701

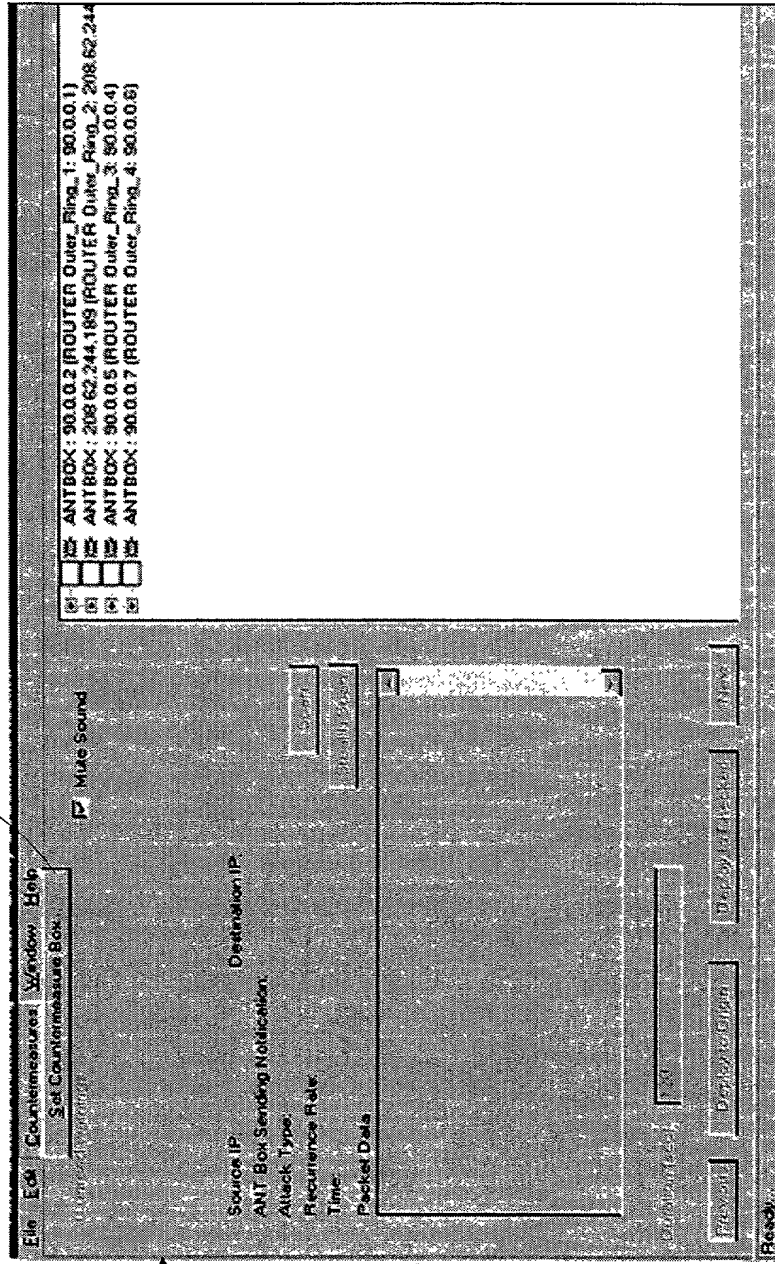


Figure 27

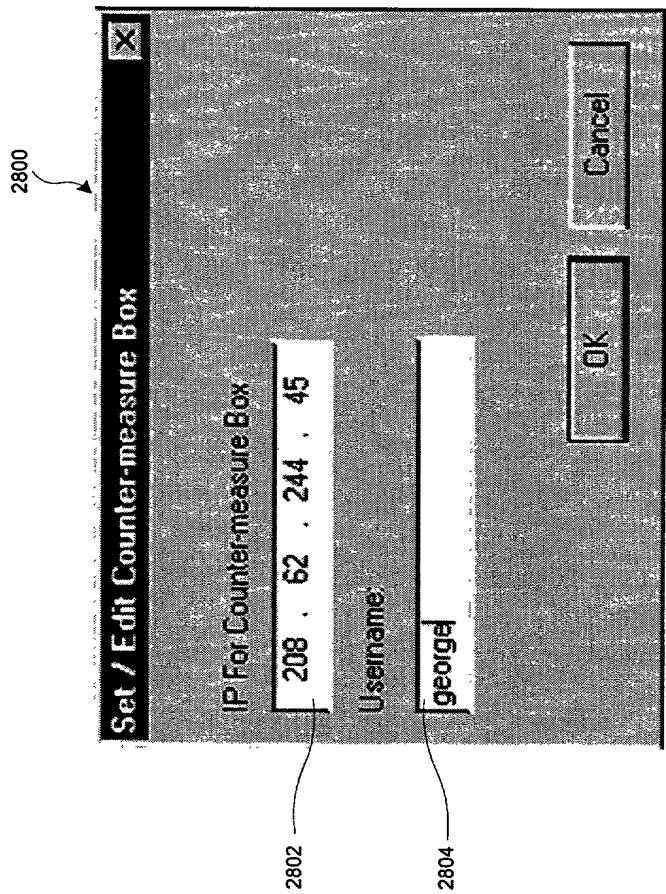


Figure 28

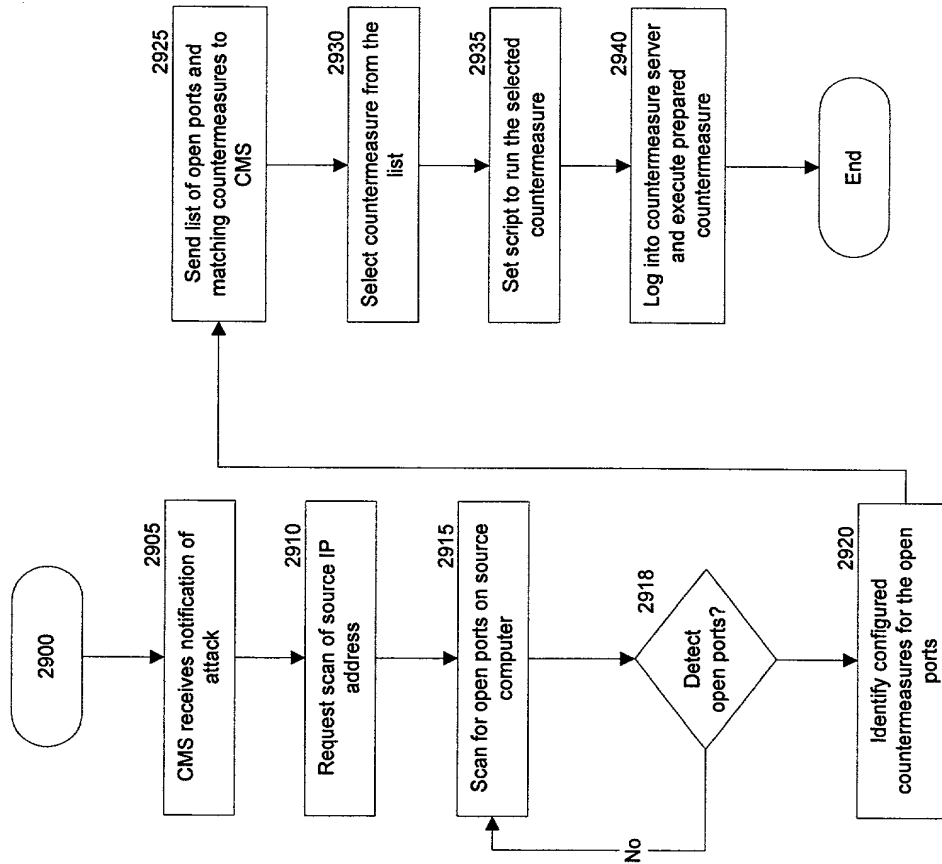


Figure 29

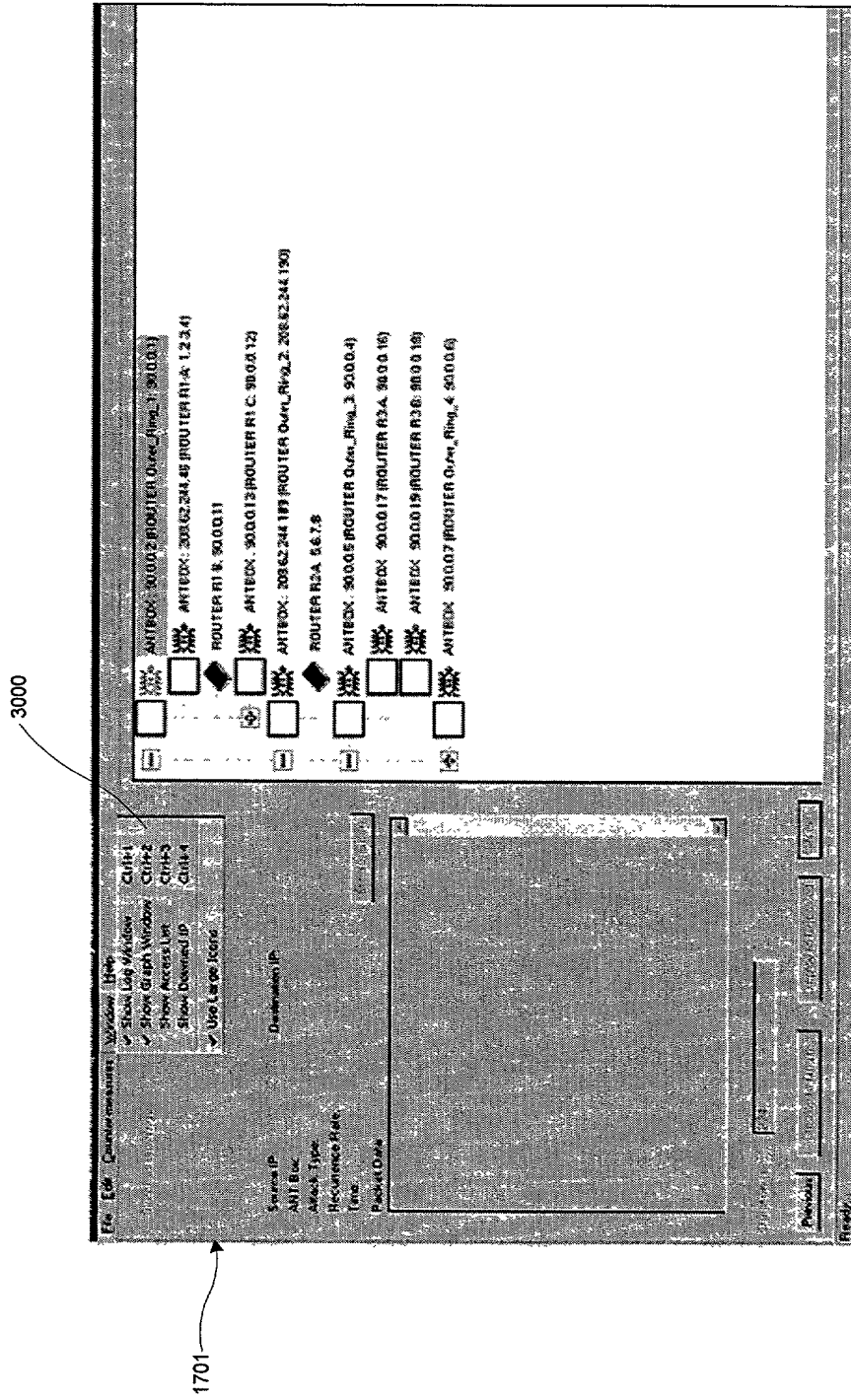


Figure 30



3200 → **Add/Edit Item** [X]

3202 Source IP: 1 . 2 . 3 . 4

3204 Source Mask: 255 . 255 . 255 . 0

3206 Target IP: 2 . 3 . 4 . 6

3208 Target Mask: 255 . 255 . 255 . 0

3210 Notes: Some hostile entity

OK Cancel

Figure 32

3300

3302

3304

3306

3300

ACL'd IP Addresses

1.2.3.4 to 5.5.5.5 IP timeout at: 1006632960  
1.1.1.2 to 2.2.2.3 IP timeout at: 1003263873  
2.2.2.2 to 3.3.3.3 TCP timeout at: 1004019930  
1.1.1.1 to 2.2.2.2 IP timeout at: 1004030052  
90.0.0.3 to 4.4.4.4 UDP timeout at: 1010700288  
1.2.3.4 to 2.3.4.5 UDP timeout at: 1010779398  
80.5.2.34 to 90.0.0.10 IP timeout at: 1011890129  
7.8.9.10 to 1.0.0.0 ICMP timeout at: 110000000  
2.2.2.2 to 4.4.4.4 IP timeout at: 1012511080  
2.2.2.2 to 4.0.0.0 IP timeout at: 1012511087

Source IP

Destination IP

Duration (seconds)

120

IP

Protocol

Add

Remove

Null Routed IP Addresses

14.15.16.17 timeout at: 1012508544

IP

Duration (seconds)

120

Add

Remove

Figure 33

3400

1701

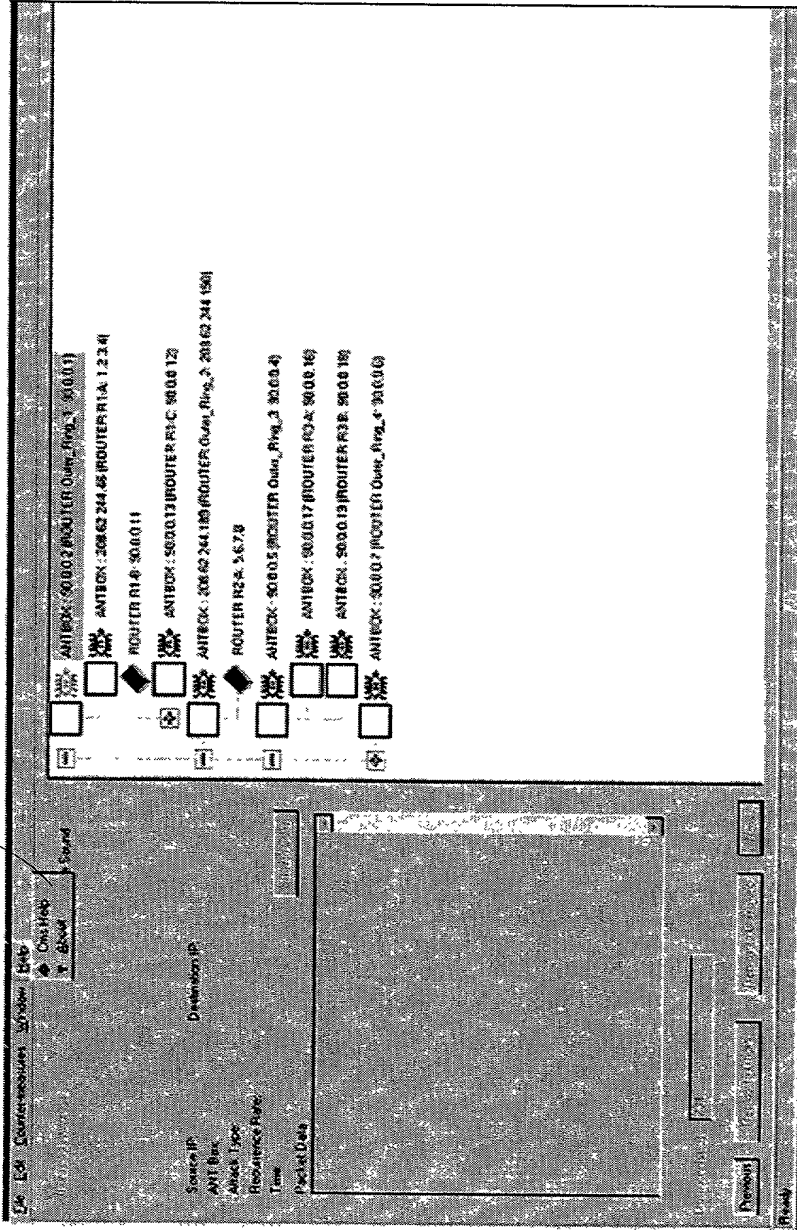


Figure 34

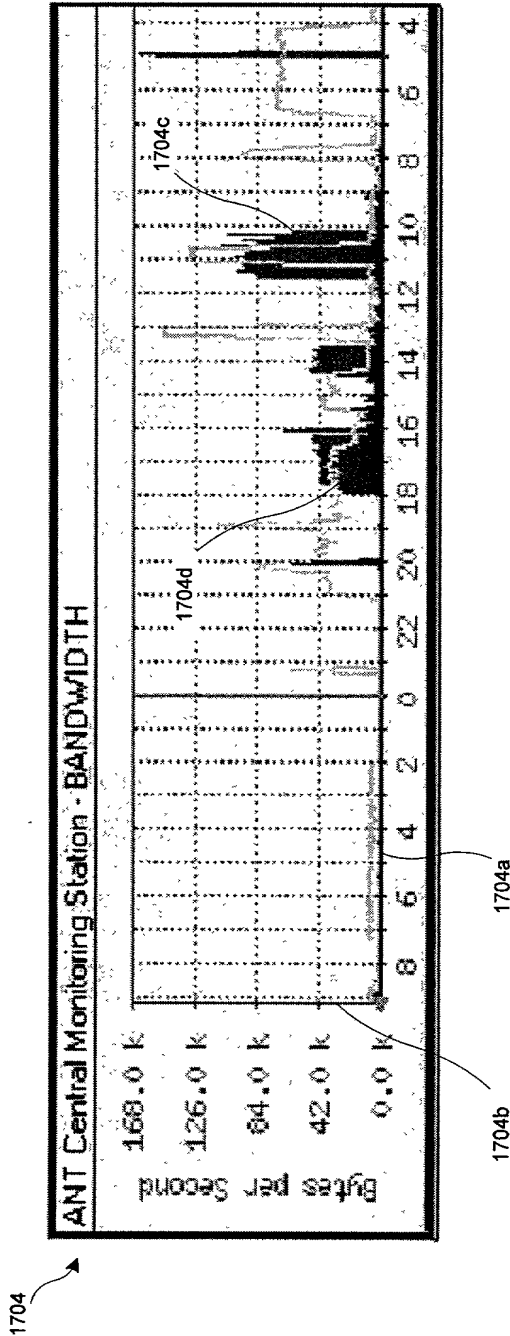


Figure 35

1702

ANT Central Monitoring Station - LOG		
[Mon Jan 31 18:22:03 EST 2002]	Countermeasure Deployed	
[Thu Jan 31 18:22:03 EST 2002]	Incoming Flood to IP: 192.168.7.255	
[Thu Jan 31 18:22:03 EST 2002]	Route Null Traffic from Source IP to Subnet Duration 5	
[Thu Jan 31 18:22:21 EST 2002]	writeacl successfully executed	
[Thu Jan 31 18:22:03 EST 2002]	Countermeasure Deployed	
[Fri Feb 1 08:23:36 EST 2002]	Incoming Flood to IP: 192.168.7.3	
[Fri Feb 1 08:23:36 EST 2002]	Route Null Traffic from Source IP to Subnet Duration 5 M	
[Fri Feb 1 08:23:54 EST 2002]	writeacl successfully executed	
[Fri Feb 1 08:23:54 EST 2002]	Countermeasure Deployed	
[Fri Feb 1 08:23:57 EST 2002]	Multiple-IP Flood to IP: 192.168.7.3	
[Fri Feb 1 08:23:57 EST 2002]	Blackholing Destination IP Duration 5 Min	
[Fri Feb 1 08:24:09 EST 2002]	writenull successfully executed	
[Fri Feb 1 08:24:09 EST 2002]	Countermeasure Deployed	
[Fri Feb 1 10:07:56 EST 2002]	Downed 192.168.7.3 -> 192.168.7.3 for 300 seconds	

Figure 36

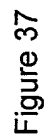
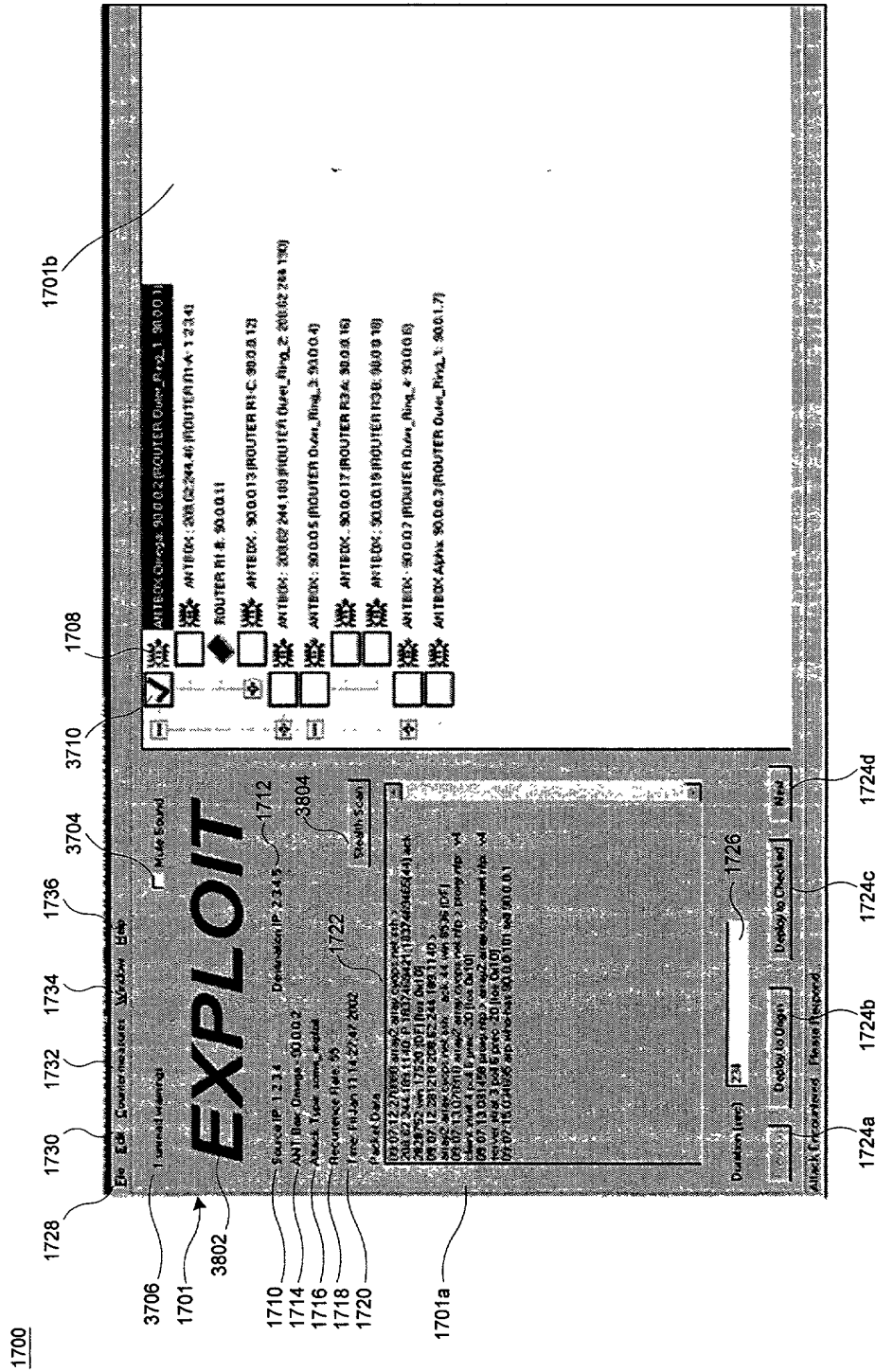


Figure 37



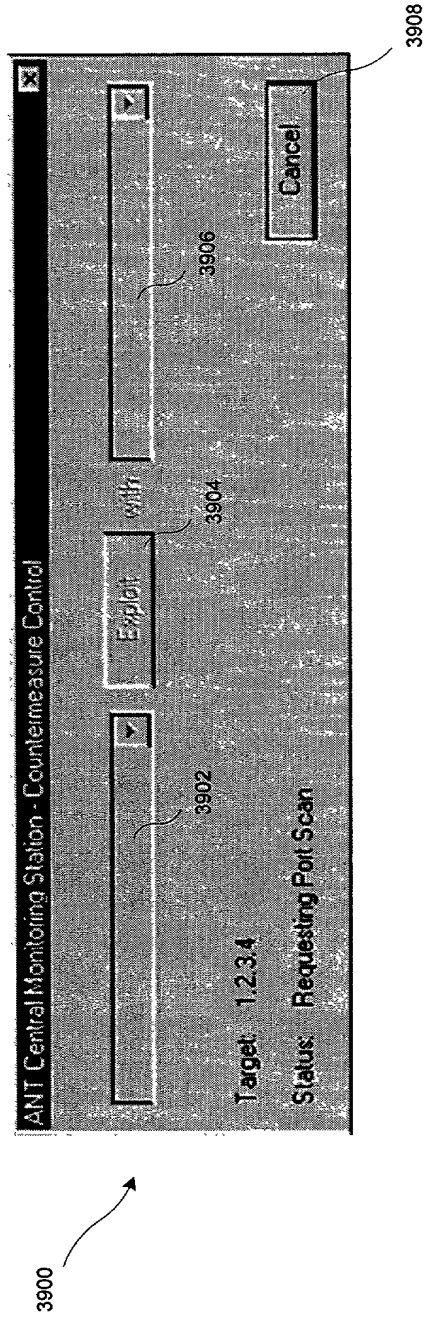


Figure 39

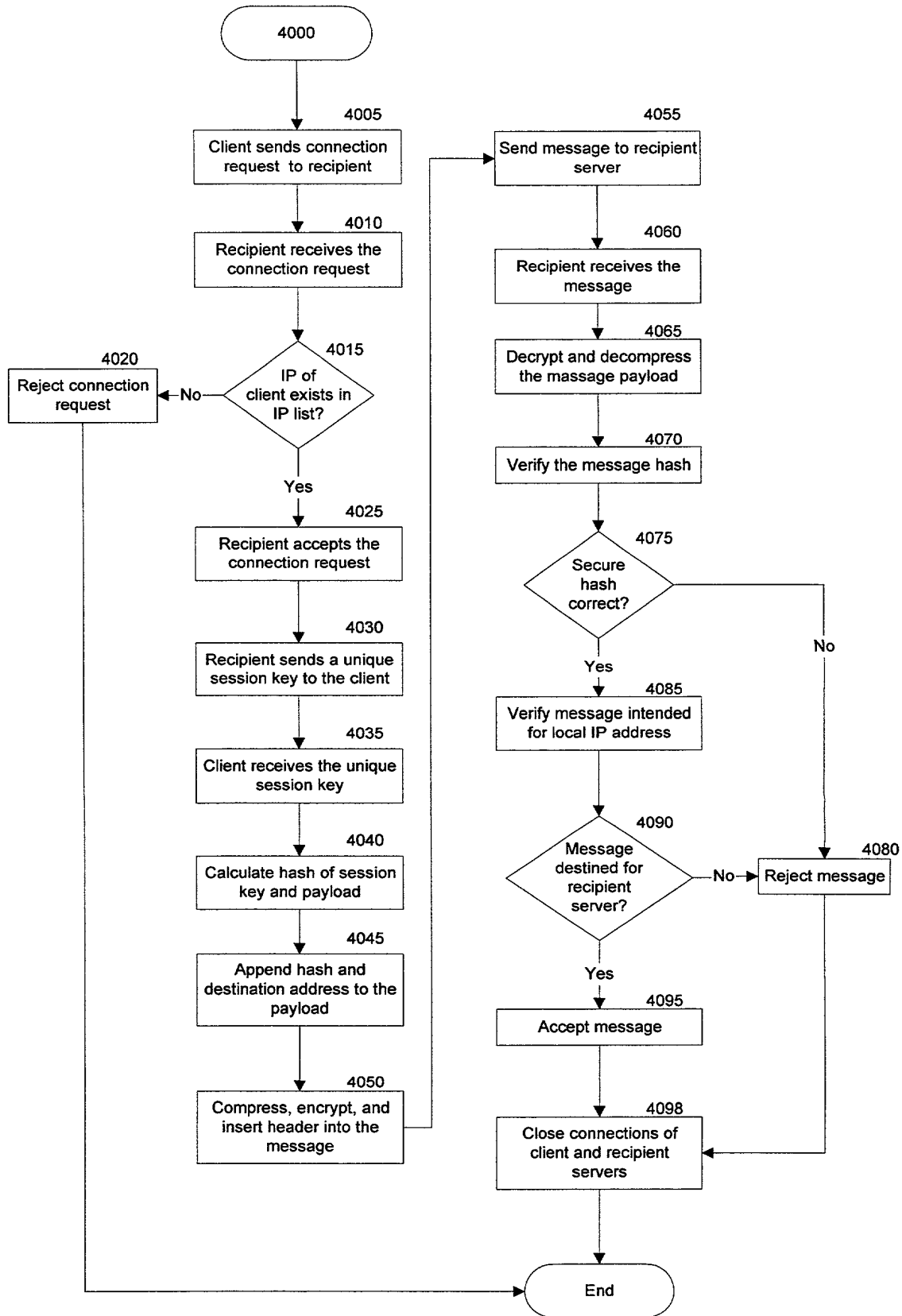


Figure 40